REMARKS

This amendment responds to the Office Action dated August 21, 2009, in which the Examiner rejected claims 20-39 under 35 U.S.C. § 103.

As indicated above, claims 20 and 32 have been amended in order to make explicit what is implicit in the claims. The amendment is unrelated to a statutory requirement for patentability.

Claims 20 and 32 claim a data transmission controlling method for controlling transmission of data from data transmitting means to data receiving means over communication channels and for causing the data transmission means to encrypt data and transmit the encrypted data to the data receiving means over the communication channels. The data transmission control method comprises the steps of first encapsulating the data having a destination address in accordance with a first protocol to form a section. The section is then encrypted. The encrypted section is then supplemented with a section header including a MAC header and a section trailer. The encrypted supplemented section is then divided into a plurality of payloads in accordance with a second protocol. Transport stream headers are added to each payload to form packets for transmission. Claim 32 recites additional features.

By (a) supplementing the encrypted sections with a section header having a MAC header and a section trailer, (b) dividing the encrypted supplemented section into a plurality of payloads and (c) adding headers to each payload to form packets for transmission, as claimed in claims 20 and 32, the claimed invention provides a data transmission controlling method which allows the data to be transmitted with related protocol requirements kept in tact and thus insuring security. The prior art does not show, teach or suggest the invention as claimed in claims 20 and 32.

Claims 20-24, 26-34 and 36-40 were rejected under 35 U.S.C. § 103 as being unpatentable over *Inoue, et al.* (U.S. Patent No. 6,163,843) and *Bhaskaran* (U.S. Patent No. 6,266,335).

Inoue, et al. appears to disclose in Figures 12A, 12B, 12C and 12D four exemplary packet formats to be processed by a packet inspection device (column 6, lines 1-3). A processing procedure related to a registration message includes using encryption of the data portion within the packet. In this example, the packet inspection device functions as a packet encryption gateway. A communication system adopts a scheme in which the link authentication is defined in conjunction with the encryption of packet content and the packet authentication between ends, as described in IEFT RFC 1825 to 1829. In the IETF, a method for attaching the authentication code to an IP packet is specified as the IP security standard (see IEFT RFC 1826, 1828), and this method is utilized here so that the authentication data between the mobile computer and the gateway of the visited network is attached to the data packet as a processing for establishing the identification of the mobile computer, and the packet is passed to the outside of the gateway after the authentication code of the received packet is checked (column 12, lines 36-57). Figures 12A to 12D show exemplary packet formats to be processed by each gateway (packet encryption gateway). Figure 12A shows a usual IP packet format. Figure 12B shows an encryption/end-to-end authentication format, which is a format for carrying out the packet encryption and authentication between end gateways or between an end gateway and the mobile computer. Figure 12C shows an encryption/link authentication format, which is to be used in a case which requires the authentication between gateways on intermediate routes or between a gateway on an intermediate route and a mobile computer. Figure 12D shows a mobile IP format, which is a

packet format to be routing controlled by the home agent into a form destined to the mobile computer (column 12, line 63-column 13, line 9).

Thus, *Inoue, et al.* merely discloses including authentication information in a packet as well as the four packet formats, containing the authentication information, which can be processed. Nothing in *Inoue, et al.* shows, teaches or suggests (a) encapsulating data, having a destination address, to form a section, (b) encrypting the section, (c) supplementing the encrypted section with a section header including a MAC header and a section trailer, (d) dividing the encrypted supplemented section into a plurality of payloads and (e) adding transportation stream headers to each payload to form packets for transmission as claimed in claims 20 and 32. Rather, *Inoue, et al.* only discloses packets containing authentication data and the four types of formats which can be processed by a gateway.

RFC 1825 at paragraph 3.2 discloses encapsulating an entire IP datagram or only an upper-layer of protocol data inside a ESP, encrypting most of the ESP contents and then appending a new cleartext IP header to the now encrypted Encapsulating Security Payload. Also disclosed at paragraph 3.1 are two cryptographic security mechanisms. The first is an Authentication Header and the second is an Encapsulating Security Payload. When the Authentication Header is used, fragmentation occurs after the Authentication Header processing.

Thus, RFC 1825 discloses two security methods, one in which fragmentation occurs after an Authentication Header processing (paragraph 3.1) and a second method using ESP in which a cleartext IP header is appended to an encrypted content (paragraph 3.2). Nothing in RFC 1825 shows, teaches or suggests (a) encapsulating data, having a destination address, as a section (b) encrypting the section, (c) supplementing an encrypted section with a section header having a MAC header and a section trailer, (d) dividing the encrypted supplemented section into a

plurality of payloads, and (e) adding headers to each payload to form packets for transmission as claimed in claims 20 and 32. Rather, RFC 1825 fragments after an Authentication Header processing, or appends a cleartext IP header to an encrypted encapsulated security payload.

RFC 1826 discloses at paragraph 1.1 Authentication Headers normally placed after fragmentation. Paragraph 3.2 discloses fields of the Authentication Header including a next header of 8 bits, a payload length of 8 bits and a reserve of 16 bits, a security parameter index of 32 bits and authentication data having an integral number of 32-bit words.

Thus, RFC 1826 discloses placing an Authentication Header after fragmentation as well as the structure of the Authentication Header. Nothing in RFC 1826 shows, teaches or suggests (a) encapsulating data, having a destination address, as a section (b) encrypting the section, (c) supplementing an encrypted section with a section header having a MAC header and a section trailer, (d) dividing the encrypted supplemented section into a plurality of payloads and (e) adding transport stream headers to each payload to form packets for transmission as claimed in claims 20 and 32. Rather, RFC 1826 only discloses the placement and structure of the Authentication Header.

RFC 1827 discloses at paragraph 3. that the Encapsulating Security Payload (ESP) may appear anywhere after the IP header and before the final transport-layer protocol. The ESP consists of an unencrypted header followed by encrypted data. Paragraph 4. discloses that ESP processing occurs prior to IP fragmentation on output and after IP reassembly or input.

Thus, RFC 1827 only discloses ESP consists of an unencrypted header followed by encrypted data and that the ESP processing occurs prior to fragmentation. Nothing in RFC 1827 shows, teaches or suggests (a) encapsulating data, having a destination address, as a section (b) encrypting the section, (c) supplementing the encrypted section with a section header having a

MAC header and a section trailer, (d) dividing the encrypted supplemented section into a plurality of payloads and (e) adding transport stream headers to each payload to form packets for transmission as claimed in claims 20 and 32. Rather, RFC 1827 only discloses an unencrypted header followed by encrypted data and subsequent fragmentation.

Bhaskaran appears to disclose the format of a packet 300 transmitted over an external network. The packet 300 has a header field 310, a link field 320, a IP header 330, a TCP header 340, a data payload 350, a CRC field 360 and a trailer 370. Header 310 and trailer 370 are 8-bit wide private tag-fields; these are not transmitted over the external network but used only inside the network flow switch (column 6, lines 26-34).

Thus, *Bhaskaran* discloses header and trailers which are only used inside the network flow switch. Thus, nothing in *Bhaskaran* shows, teaches or suggests that the section header and trailer will be divided into payloads, and the payload will have transport stream headers added thereto before being transmitted as claimed in claims 20 and 32. Rather, *Bhaskaran* teaches away from the claimed invention since the header and trailers are not transmitted over an external network and are only used inside the flow switch.

Furthermore, *Bhaskaran* only discloses the format of the packet. Nothing in *Bhaskaran* shows, teaches or suggests (a) encapsulating data, having a destination address, as a section, (b) encrypting the section resulting from the encapsulation, (c) supplementing the encrypted section with a section header having a MAC header and a section trailer as claimed in claims 20 and 32. Rather, *Bhaskaran* only discloses the format but does not show, teach or suggest how the format is formed.

A combination of *Inoue, et al.* and *Bhaskaran* would merely suggest to include authentication information within a packet as taught by *Inoue, et al.* and RFC 1825-1827 and to

have headers and tailers which are not transmitted but only used inside a flow switch as taught by *Bhaskaran*. Thus nothing in the combination of the references shows, teaches or suggests how the data packet is formed and in particular does not show, teach or suggest (a) encapsulating data, having a destination address, to form a section, (b) encrypting the section, (c) supplementing the encrypted section with a section header having a MAC header and section trailer, (d) dividing the encrypted supplemented section into a plurality of payloads according to a second protocol and (e) adding transport stream headers to each payload to form packets for transmission as claimed in claims 20 and 32. Therefore, Applicant respectfully requests the Examiner withdraws the rejection to claims 20 and 32 under 35 U.S.C. § 103.

Claims 21-24, 26-31, 33-34 and 36-39 depend from claims 20 and 32 and recite additional features. Applicant respectfully submits that claims 21-24, 26-31, 33-34 and 36-39 would not have been obvious within the meaning of 35 U.S.C. § 103 over *Inoue et al., Bhaskaran* and RFC 1825 – 1827 at least for the reasons as set forth above. Therefore, Applicant respectfully requests the Examiner withdraws the rejection to claims 21-24, 26-31, 33-34 and 36-39 under 35 U.S.C. § 103.

Claims 25 and 35 were rejected under 35 U.S.C. § 103 as being unpatentable over *Inoue et al.* and *Bhaskaran* and further in view of *Takeda et al.* (U.S. Patent No. 6,178,244).

Applicant respectfully traverses the Examiner's rejection of the claims under 35 U.S.C. § 103. The claims have been reviewed in light of the Office Action, and for reasons which will be set forth below, Applicant respectfully requests the Examiner withdraws the rejection to the claims and allows the claims to issue.

As discussed above, since nothing in *Inoue et al.* and *Bhaskaran* shows, teaches, or suggests the primary features as claimed in claims 20 and 32, Applicant respectfully submits that

the combination of the primary reference with the secondary reference to *Takeda et al.* will not overcome the deficiencies of the primary reference. Therefore, Applicant respectfully requests the Examiner withdraws the rejection to claim 25 and 35 under 35 U.S.C. § 103.

Thus, it now appears that the Application is in condition for reconsideration and allowance. Reconsideration and allowance at an early date are respectfully requested.

CONCLUSION

If for any reason the Examiner feels that the application is not now in condition for allowance, the Examiner is requested to contact, by telephone, the Applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this case.

In the event that this paper is not timely filed within the currently set shortened statutory period, Applicant respectfully petitions for an appropriate extension of time. The fees for such extension of time may be charged to Deposit Account No. 50-0320.

In the event that any additional fees are due with this paper, please charge our Deposit Account No. 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicant

Date: November 18, 2009

By: _____
Ellen Marcie Emas
Reg. No. 32,131
(202) 292-1530